**Juniper Networks
Steel-Belted Radius**

Release Notes

Release 6.1.1
June 2009

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Revision History

Date	Description
16 June 2009	Third update to Steel-Belted Radius Release 6.1.1 release notes (documentation corrections)
21 January 2009	Second update to Steel-Belted Radius Release 6.1.1 release notes (limited Windows Vista support)
19 November 2008	First update to Steel-Belted Radius Release 6.1.1 release notes (32-bit support)
27 October 2008	Initial release of Steel-Belted Radius Release 6.1.1 release notes.
20 December 2007	Second release of Steel-Belted Radius Release 6.1 release notes.

M09616

Table of Contents

Release Notes
Steel-Belted Radius Release 6.1.1

These release notes accompany Release 6.1.1 of the Steel-Belted Radius software. Before you install or use your new software, you should read these release notes in their entirety, especially the "Known Problems and Limitations" section on page 6.

If the information in these release notes differs from the information found in the product documentation, follow these release notes.

You can find these release notes in Adobe Acrobat (PDF) format on the Juniper Networks Technical Publications Web page, which is located at http://www.juniper.net/techpubs/software/aaa_802/sbr.html.

Product information for Steel-Belted Radius can be found at http://www.juniper.net/products_and_services/aaa_and_802_1x/ steel_belted_radius/.

System Requirements

SBR Administrator

The web-deployed SBR Administrator can co-exist with previous versions of the SBR Administrator software. They do not affect one another.

Solaris

Release 6.1.1 of the Steel-Belted Radius software runs on Sun Solaris 9 (SPARC Platform Edition 8/03 or later) or Sun Solaris 10 (SPARC Platform Edition 3/05 or later) on an UltraSPARC processor.

■ The JDBC plug-in has been tested with these databases: MySQL running on Solaris or Linux, Oracle running on Solaris or Linux, and MSSQL.

■ On Solaris 9 and 10, the SBR Administrator works with either of two desktop managers: Gnome2-metacity or CDE-dtwm.

■ The watchdog program, radiusd, (also referred to as the Auto Restart Module) requires perl 5.8.3. Earlier and later perl versions may cause problems. You must edit the first line of the radiusd script to specify where perl 5.8.3 is installed.

Before You Install on Solaris

Before upgrading the Steel-Belted Radius software, you must stop the Steel-Belted Radius server and create an archive copy of your \radius directory. This will allow you to migrate items such as certificates, JRE extensions, and SNMP configuration information, which are not automatically migrated by the conversion script, after you have completed the upgrade steps. (8644)

Operating System Patches – Solaris 9

The following patches (or better) are required for Solaris 9:

- 112963-25 ld.so.1

- 111711-16 libC 32-bit

- 111712-16 libC 64-bit

- 117560-03 libmtsk

- 111722-05 libm

- 115697-02 mtmalloc

The following patches (or better) are recommended, but not required, for Solaris 9:

- 112785-56 X11 6.6.1: Xsun

- 113886-28 OpenGL 1.3 32-bit for J2SE

- 113887-28 OpenGL 1.3 64-bit for J2SE

- 113096-03 X11 6.6.1: OWconfig for J2SE

Be sure to obtain your patches directly from Sun (www.sun.com), review the patch README files, and consider making a backup before altering your system.

Operating System Patches – Solaris 10

The following patches (or better) are required for Solaris 10:

- 120900-04 libzonecfg

- 121133-02 zoneadm

- 119254-28 patchadd

- 119578-22 FMA patch for J2SE

- 118822-30 kernel patch for J2SE

- 118833-24 kernel patch

- 120753-02 libmtsk

- 119963-07 libC

The following patches (or better) are recommended, but not required, for Solaris 10:

- 121620-02 MediaLib

Be sure to obtain your patches directly from Sun (www.sun.com), review the patch README files, and consider making a backup before altering your system.

Linux

Release 6.1.1 of the Steel-Belted Radius software runs on the 32-bit versions of Red Hat Enterprise Linux ES or AS 4.0 and Red Hat Enterprise Linux ES or AS 4.5. Release 6.1.1 does not run on 64-bit versions of Linux.

■ The system must have glibc 2.3.2 or 2.3.3 for Red Hat 4.0 or 4.5 ES or AS. The rpm installer may direct you to obtain a compatibility package from the vendor.

■ Birdstep database (RDMe) replaces the BTrieve database. If you are migrating data from a previous version installation, you must convert your database per the instructions in the *Steel-Belted Radius Installation and Upgrade Guide*.

■ The watchdog program, radiusd, (also referred to as the Auto Restart Module) requires perl 5.8.3. Earlier and later perl versions may cause problems. You must edit the first line of the radiusd script to specify where perl 5.8.3 is installed.

■ The JDBC plug-in has been tested with these databases: MySQL running on Solaris or Linux, Oracle running on Solaris or Linux, and MSSQL.

Before You Install on Linux

■ Before upgrading the Steel-Belted Radius software, you must stop the Steel-Belted Radius server and create an archive copy of your \radius directory. This will allow you to migrate items such as certificates, JRE extensions, and SNMP configuration information, which are not automatically migrated by the conversion script, after you have completed the upgrade steps. (8644)

■ When upgrading the software, do not use the -U option of rpm. Refer to the *Steel-Belted Radius Installation and Upgrade Guide* for more information.

■ If you are migrating data from a previous version of Steel-Belted Radius, you must convert your database per the instructions in the *Steel-Belted Radius Installation and Upgrade Guide*.

Windows

Release 6.1.1 of the Steel-Belted Radius software runs on the 32-bit version of Windows XP or Windows Server 2003. Release 6.1.1 does not run on 64-bit versions of Windows.

■ Service Pack 2 is required for servers running Windows XP.

■ Steel-Belted Radius does not coexist with the RADIUS server installed with RSA Authentication Manager Version 6.1 or later. You can upgrade RSA RADIUS to Steel-Belted Radius release 6.1.

Before You Install on Windows

If you are migrating data from a previous version of Steel-Belted Radius, you must convert your database per the instructions in the *Steel-Belted Radius Installation and Upgrade Guide.*

Steel-Belted Radius Appliance

Contact your sales representative concerning the availability of Steel-Belted Radius Appliance Release 6.1.1.

Supported Browsers

The SBR Administrator configuration application can be launched from the browsers listed in Table 1.

Table 1: Supported Browsers

Operating System	Supported Browsers
Solaris 9	Mozilla Firefox 1.5–1.7 and 2.0
	Netscape Navigator 6.00, 7.*x,* and 8.1
Solaris 10	Mozilla 1.7
	Mozilla Firefox 1.5–1.7 and 2.0
	Netscape Navigator 6.00, 7.*x,* and 8.1
Red Hat Linux ES and AS 4.0	Mozilla Firefox 1.0, 1.5–1.7, and 2.0
Windows XP	Microsoft Internet Explorer 6.0, 6.1, and 7.0
	Mozilla Firefox 1.5–1.7, 2.0, and 2.0.0.1
	Netscape Navigator 7.*x* and 8.1
Windows Vista	Microsoft Internet Explorer 7.0
	Mozilla Firefox 1.5–1.7, and 2.0
	Netscape Navigator 7.*x* and 8.1
Windows Server 2003	Microsoft Internet Explorer 6.0, 6.1, and 7.0
	Mozilla Firefox 1.5–1.7, 2.0, and 2.0.0.1
	Netscape Navigator 7.*x* and 8.1

Java Runtime Environment (JRE) 1.4.2 or newer is required for all browsers, and is available from http://java.sun.com.

To view an audit log, use the following browsers:

- Mozilla Firefox 1.5–1.7 and 2.0

- Microsoft Internet Explorer 6.0, 6.1, and 7.0

Database Servers

The following databases are recommended for use with the Steel-Belted Radius server running on Solaris or Linux using JDBC or running on Windows using ODBC:

- Oracle 8.1.7

- Oracle 9.2.0

- Oracle 10.2.0

- MS-SQL Server 2000 8.0.2039

- MS-SQL Server 2005 9.0.1399

- MySQL 5.0.27

The following databases are recommended for use with the Steel-Belted Radius server running on Solaris using native Oracle plug-ins:

- Oracle 8.1.7

- Oracle 9.2.0

- Oracle 10.2.0

Database Clients

- If you use Oracle stored procedures on a Steel-Belted Radius server running Windows, choose the Oracle 9i client.

- If you are running Steel-Belted Radius on a Solaris server and using an Oracle database and a native Oracle plug-in, the Steel-Belted Radius server can use any Oracle 8, 9, or 10 client. However, Oracle 8.1.7, 9.2.0, and 10.2.0.3 are recommended.

NOTE: Oracle 10 typically requires a patch for Oracle bug 4516865 to correct the installed Oracle file access modes.

New Features and Enhancements

Release 6.1 of the Steel-Belted Radius software includes the following changes:

- Standards-based login communication—SBR Administrator uses HTTPS instead of a proprietary protocol for login requests. If the Steel-Belted Radius server does not have a current server certificate, the server generates a new self-signed server certificate.

- Certificate revocation list (CRL) cache and proxy enhancements—Certificate processing has been improved in Release 6.1 in several respects:

  - Support for CRL cache flushing

- CRL cache timeout

- Enforcement of CRL serial numbers

- CRL proxy connection settings

- Proxy exclusion list

- Static CDPs

- CCM replication

- Support for background CCM replication

- Replication backup and restore

- Daylight savings time—Release 6.1 adds support for automatic adjustment of system clock for daylight savings time. Additionally, users can choose between local time and UTC (coordinated universal time) for timestamps in the event log file.

- Configurable error handling for backend databases—Users can now specify whether errors should cause a disconnect/reconnect to a MySQL, ODBC, or Oracle database.

- Steel-Belted Radius is now based on the Birdstep RDMe database. Users who are upgrading from previous releases of Steel-Belted Radius may have to do some manual data conversion depending on the operating system they are running.

☞ **NOTE:** On Windows platforms, the database migration only works when the upgrade is performed as a console connection. If you are upgrading via an RDP (Remote Desktop) non-console connection, the automatic database migration will fail. Refer to the *Steel-Belted Radius Installation and Upgrade Guide* for details.

- Operating system changes— Release 6.1 drops support for RedHat Linux ES/AS version 3.*x* and for all versions of SuSE Linux.

Known Problems and Limitations

The following issues have been identified in the Steel-Belted Radius release 6.1.1 software. The identifier in brackets is the tracking number in our bug database.

- **Key for directed realms appears to be for older version**—When a key for additional directed realms is entered through the Administrator, a popup will appear warning that the license is for an older version. However, the key is valid and will take effect upon restart of SBR. (261257)

- **Using filters with multiple realms**—Since realm filters are cumulative, they will be applied to successive accounting realms. As a workaround, use the Block = 0 option in the realms' .pro files. (247515)

- **Changing Primary status with SBR Administrator**—If the SBR Administrator is used to modify the configuration, the Primary status does not reflect the modification until the configuration is published. (247862, old ID-6428)

- **Editing record types on Replicas**—Although it appears you can modify the Replica configuration using the SBR Administrator, Replica configuration changes are overwritten by the Primary when the Primary configuration is published. (247873)

- **Browsing UNIX groups with SBR Administrator**—When browsing UNIX groups, in the users list using the SBR Administrator, not all groups are listed if one group is particularly large. The workaround for this issue is to add groups manually and to use multiple smaller groups. (247925)

- **Conflicting attribute values in dictionaries**—Values displayed for attributes may not be consistent if they are defined in multiple dictionaries. If this happens, delete or modify one of the conflicting dictionaries. (249476)

- **Creating Replica servers with no name**—If a Replica server is created without a Name, it cannot be edited, enabled, or deleted. When creating Replica servers through the SBR Administrator, always enter a server name in the Name field. (249531)

- **SNMP get issue**—SNMP gets no longer function if TcpControlAddress is changed in radius.ini. Do not modify this setting for CCM if are you using SNMP. (257797)

- **Using the MasterDictionary feature may add/allow unknown attributes**—If you specify MasterDictionary=1 in radius.ini, two of your vendor-specific dictionaries associate a particular attribute number with different types (such as string and int). Therefore, the attribute value that Steel-Belted Radius sends may be incorrect. It is recommended that you specify MasterDirectionary=0. (248476, old ID-7217)

- **Misleading error message when Maximum Open Tunnels value is not set**—When configure a tunnel but do not set Maximum Open Tunnels for the tunnel, you may see the following error message: 04/27/2006 03:11:27 Failed to decrement usage count for CINGULAR.COM as it no longer exists. It is recommended that you set a Maximum Open Tunnels value. You can make this a large value to avoid possible issues. (248650, old ID-7458)

- **Missing Audit Log entries for Replicate Trusted Root Certificate changes**—If you enable auditing and then you check or uncheck the Replicate Trusted Root Certificates checkbox in the Trusted Root Certificates panel, the audit log will not contain record of this change. (249480, old ID-8420,8380)

- **Missing Audit Log entries for added license keys**—If you enable auditing and then add a license key using SBR Administrator, the audit log will not contain record of the new license. (249438)

- **Notify and Publish events are identical**—When you perform a Notify on the Replication panel, the event that is logged appears identical to a Publish event. (You see <writeEvent object="/CCM/publish/">PUT /CCM/publish/</writeEvent>.) (248814)

- **No stored procedures with MySQL**—As of MYSQL 5.0 and 5.1, stored procedures are supported by MYSQL and can be used with Steel-Belted Radius when using a SQL backend for authentication and accounting. Note that there are known issues with MYSQL when using CALL statements such as "SQL = {call rsp_getpword (%username!i, %password!o)}". However, execute statements, such as "SQL = Execute rsp_getpword %username, %password" work fine. See MYSQL for further details. (8130)

Resolved Issues

The following issues from previous releases have been resolved in the Steel-Belted Radius release 6.1 software. The identifier in brackets is the tracking number in our bug database.

Problems Resolved in Release 6.1.1

- SNMP get requests fail when a TcpControlAddress is configured in radius.ini. (255899)

- LDAP authentication fails when simultaneous authentications are attempted. (258354)

- LDAP authentication fails due to login limit exceeded when using routed proxy. (260680)

- Proxy target statistics are incorrect in the SBR administrator. (261108)

- Server crashes when stripping usernames. (262371)

- LDAP authentication does not work against Microsoft when searching the top base. (269036)

- The "block = 1" setting does not work for static accounting realms. (271743)

- Machine authentication fails when username contains a DNS subdomain. (273069)

- Native user passwords can not contain international characters. (276427)

- Server crashes when LDAP authentication is configured on Linux. (278229)

- EAP-Id is incremented in accept packet for LEAP authentication. (281842)

- RSA SecurID authentication fails because of socket leak. (282087)

- Client shared secrets are not propagated to replica servers. (282975)

- Server crashes when a native user record is accessed in the SBR Administrator. (284066)

- The stringnz attribute type is not working for response attributes configured with HiddenEAPIdentity in radius.ini. (286845)

- Calling software development kit function **SbrCtrlEnumResponseAttributes**() in a plugin causes enumerated attributes to be removed from response. (287519)

- When using SQL accounting, not all values of multivalued attributes are inserted in the database. (288198)

- SBR sends cached response for duplicate request. (289089)

- Server crashes when client deleted. (295621)

- Setting stringnz for State attribute in radius.dct does not disable null termination of the attribute. (297203)

- SBR uses vulnerable version of zlib. (297217)

- The service type mapping feature does not conform to client IP address ranges. (297755)

- MS-CHAPv2 authentication fails against a native mode Windows Server 2008 domain. (298140)

- The authentication reports reject log does not specify rejects due to lockout. (300360)

- Server crashes during shutdown when Java scripting enabled. (302686)

- SBR is utilizing large amounts of memory when using CRL checking. (304075)

- Server crashes when JDBC plugin enabled. (305992)

- LEAP-MS-CHAPv2 authentication fails against Windows Server 2008. (307733)

- Server hangs if disk full while processing accounting carryover. (310055)

Problems Resolved in Release 6.1

- **Directed realms**—If you configure more than 10 directed realms, the extended directed realm license key is not recognized, limiting the number of directed realms to 10. (249828, old ID-8789)

- **Duplicate entries in filters.ini**—If the filters.ini file contains duplicate filter names, the Filter panel will hang. This should only occur when users upgrade from pre 6.0 SBR releases to 6.1. If users encounter this issue, they should verify in their filter.ini that there are no duplicate filter names. If this does not solve the issue, contact JTAC. (249833, old ID-8794)

- **Current sessions in LCI**—If you use the LCI to display current sessions on Windows or Linux, Framed-ip-address attributes are displayed in reverse byte order. (249818, old ID-8780)

- **Enabling a replica server**—If you connect SBR Administrator to the primary server, you click **Add** in the Replication panel to add a replica, and then click the Enable check box in the Add dialog, the new setting for Enable may be discarded after you click OK. If this occurs, use the **Enable** check box on the Edit dialog. (249497, old ID-8438)

- **Upper-case characters in filters.ini**—If the filters.ini file contains upper-case characters in filter names, the radio button on the Edit Rule panel will be uninitialized. If this occurs, change the case of all filter names to lower case. (249838, old ID-8799)

- **Name of Location Group**—The names of location groups are case-sensitive. You should ensure that the case of a location group name used in the JNPRsbr-Radius-Client-Group checklist attribute matches the case used in the Location Groups panel. (249675, old ID-8627)

- **Rulesets setting in admin.ini** (GEE)—If your admin.ini file contains an AccessLevel section that specifies Certificates = r or Certificates = rw, but does not specify RuleSets = r or RuleSets = rw, then when an administrator with that access level navigates to the Trusted Root Certificates or Certificates panels in SBR Administrator, a Validation Error message box displays the following:

  </pre></BODY></HTML>

  This is likely to occur after an upgrade. To resolve this problem, add RuleSets=r to the definition of the AccessLevel, and restart the Steel-Belted Radius server. (249567, old ID-8516)

- **"Certificate Expiration Warning" value**—If you try to change the certificate expiration warning from the default of 30 days in the Certificates panel of SBR Administrator, a "Validation Error" message appears. You should accept the default of 30 days. (8524)

- **Reports access setting** (GEE)—If the (Reports) section of admin.ini is inactive or specifies CurrentUsers=r, then an administrator with the Reports access level will not be able to use the Current Sessions panel.

  To resolve this problem:

  - Uncomment (remove the semi-colon) the (Reports) section of admin.ini

    (Reports)

  - Uncomment the CurrentUsers setting and change its value to rw:

    CurrentUsers=rw

  - Restart the Steel-Belted Radius server. (8535)

- **Inconsistent permissions in access.ini** (GEE)—If you remove a right from one of the sections of access.ini (for example, if you delete Profiles=r in the (Users) section or you create a new section with a freely chosen set of rights), then when an administrator goes to a panel where he or she has some but not all of the required access rights, a Validation Error message box displays the following:

  </pre></BODY></HTML>

  To resolve this problem, do not alter the original sections of admin.ini. Instead, create new sections as needed by adding together the rights in some of the original sections. Take the union of the rights. For example, administrators who visit the Users panels must have at least the Profiles=r right. (8590)

- **Large Windows domain** (Windows only)—If your Windows domain has thousands of users and you click **Add** in the Administrators panel, SBR Administrator may take many minutes for the available usernames to appear. During this time, the Steel-Belted Radius server does not respond to other copies of the SBR Administrator.

  To avoid this problem, create a local Windows group with a name such as **sbradmins**. Add this group to **access.ini.** Restart Steel-Belted Radius. Add administrators to the **sbradmins** group. (8480)

- **EAP Methods panel**—If you go to the EAP Methods panel, make a change, and then go elsewhere, an Unexpected Error message may appear. If this occurs, return to the EAP Methods panel, click **Refresh**, and verify that your changes appear correctly. (8454)

- **Problems deploying SBR Administrator**—If you start up the SBR Administrator normally - especially with a new version or a new server, you may occasionally see a **deployer.exe has encountered a problem and needs to close** or **invalid signature** error message. (8294)

  If you are running the SBR Administrator on Windows:

  1. Exit all copies of your Web browser,

  2. Open a Windows file browser,

  3. In the address bar, enter **%APPDATA%**,

  4. Double-click **Juniper Networks**,

  5. Select **WebDeployer** and delete it.

  If running SBR Administrator on Solaris or Linux:

  1. Exit all copies of your Web browser,

  2. In a shell, enter

     rm -rf ~/.junipernetworks/WebDeployer

- **Secondary Authentication**—If you check **Include Certificate Information** under the Secondary Authentication tab for the EAP-TLS helper authentication method, then the related Funk VSAs Funk-Peer-Cert-Hash, Funk-Peer-Cert-Issue, Funk-Peer-Cert-Principal, and Funk-Peer-Cert-Subject are not added to the request. To resolve the problem, edit the *$RADIUSDIR*/system/translators/tlsauth.eap.xml file to read <object id="Include_Certificate_Info" type="boolean" default="false"(249799, old ID-8757)

- **Admin root certificates**—If you import a root certificate with a key size larger than 2048 is imported, the SBR Administrator reports that the certificate is invalid. If this occurs, place the certificate in the ROOT directory; it won't show up in SBR Administrator, but it will be available for use by TLS and TTLS.(8754)

- **Windows Installer must be told server's role during upgrade**—When you upgrade from a previous release of Steel-Belted Radius, the installer does not remember whether the host was a standalone server, a primary server, or a replica server. If you give a different answer during the upgrade, results are unpredictable. To avoid this, enter the same answer (standalone, primary, or replica) as before. (8587)

- **SBR Administrator may reject a valid license**—If you enter a license key using the SBR Administrator License menu, you may see a message similar to Registration failed - '1634 xxxx xxxx xxxx xxxx xxxx xxxx' is not compatible with this edition of product, even if your license key is compatible with the edition of the product. If this occurs, use a text editor to open the radius.lic file and remove any licenses belonging to other editions. Add the new license key. Restart Steel-Belted Radius. (8550)

- **Configuring Oracle**—If you configure SBR on a Solaris computer with an Oracle 9.2 client, the configure script prompts for the path of the Oracle shared libraries:

      Enter path for Oracle shared libraries (/app/oracle/lib):

  The default response will not work in some cases, because Oracle has moved certain 32-bit Oracle libraries to a new subdirectory. Because they are not being will not be found. the server will not start. (8446)

  To avoid this problem, reply to the prompt, replacing the default /lib response with /lib32:

      Enter path for Oracle shared libraries (/app/oracle/lib): **/app/oracle/lib32**

- **Import**—If you export an SBR server's database and then import the data into another SBR server, the order of ordered, multi-valued attributes such as Calling-Station-ID may be changed. This only occurs if there are more than nine values. This does not affect most customers. If this occurs, consider using the LDAP Configuration Interface to move such items. (8440)

- **Publishing**—If the scripts directory contains files larger than about 25KB, publishing can take minutes. Avoid very large scripts. (8536)

- **Editing certificate information on a replica server**—If the SBR Administrator is connected to a replica server and you make a change in the Certificates panel, the change may not be not saved, and a message box displays the following:

      </pre></BODY></HTML>

  To resolve this problem, modify the certificate information on the primary server. (8523, 8525)

- **Replicate Certificate check box**—If the SBR Administrator is connected to a primary server and you check **Replicate Certificate** in the Certificates panel before you install a certificate, an Error 500 error message appears. If this occurs, add a certificate and then check **Replicate Certificate**. (8505)

- **Statistics for replica server**—If you connect the SBR Administrator to the primary server, open the **Statistics:System** panel, and select a replica server to view, the replica server statistics may not appear. If this occurs, connect the SBR Administrator to the replica of interest and open the **Statistics:System** panel. (8558)

- **Statistics for replica server**—If you connect the SBR Administrator to a replica server and open one of the Statistics panels, the replica server statistics may not appear. If this occurs, select the name of the replica server in the **Server:** drop-down list. When the name of the replica server appears, click it. (8558)

- **Startup of a replica server**—If you start a replica server when the primary is unreachable, the replica server may fail to start. Contact Technical Support for a workaround. (8434)

- **SNMP** (Solaris/Linux only)—If you are running the Steel-Belted Radius SNMP agent on a multihomed host, the value of the agent address SNMP attribute may differ from the actual source IP address when the agent sends traps or alarms. (7227)

- **LDAP Authentication**—If you SSL for LDAP authentication, Steel-Belted Radius may crash. If this occurs, contact Juniper Technical Support. (8729)

- **Online Help**—If Internet Explorer is your default browser and you use the default security settings for Windows XP SP2, Internet Explorer blocks the online help for SBR Administrator and displays the following message:

  To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer.

  To display the online help for SBR Administrator, click the option to allow blocked content. If a security warning appears, confirm you want to open the online help file.

  If you want to allow online help for SBR Administrator to run without being blocked, you can select **Tools > Internet Options > Advanced** Tab in Internet Explorer and click the **Allow active content to run in files on My Computer** check box. Consult your network administrator before making this change to your security settings. (249594, old ID-8545)

- **Configuring a replica's certificate if the primary is replicating its certificate**—If the primary is replicating certificates (checkbox on "Certificates" panel), then on replicas of that primary, the "Certificates" panel should be read-only. (249627, old ID-8576)

- **Administrator controls are active on replica's Certificates panel**— (249550, 249554, old ID-8499, 8503)

- **Routed proxy with EAP/MS-CHAP-V2**— When performing a routed proxy with EAP/MS-CHAP-V2, the value for %ProxyUserName must be in all upper case characters or the authentication is rejected. (249471, old ID-8411)

- **SBR Administrator does not work with Netscape Communicator 4.78, the default browser on Solaris 9**— (249130, old-ID 8053)

- **SBR Administrator rights in the Tunnels panel**—SBR Administrator users are able to edit the controls on the Name Parsing tab of the Tunnels panel in the Administrator application when they should not have the privileges to do so. (248563, old ID-7335)

Problems Resolved in Release 6.0.1

Steel-Belted Radius release 6.0.1 corrects a problem in which Steel-Belted Radius could exhaust all threads under conditions of extremely heavy load. (8790)

Problems Resolved in Release 6.0.0

- Steel-Belted Radius now supports Accounting files greater than 2GB. (8304)

- A USR2 signal could hang Linux Steel-Belted Radius if JDBC-SQL was not enabled. (8285)

- Accounting routed proxy did not preserve response attributes. (8114)

- A vulnerability in OpenSSL (see http://www.openssl.org/news/secadv_20060905.txt) has been resolved. (7907)

- Support for SQL "dynamic cursors" has been added. (7832)

- A problem where performing ldapcompare operations against the LCI could cause a segmentation fault has been resolved. (7831)

- EAP-Identifier was incorrectly incremented in EAP-Success messages. (7829)

- In LDAP authentication, onFound after onNotFound didn't work. (7823)

- Support has been added for sunmd5 password encryption. (7815)

- Support has been added for DHCP option 61. (7677)

- Support has been added for single-octet (int1) checklist attributes. (7676)

- TLS CRL cache files were not deleted. (7615)

- Several dictionaries (hpprocurve, nokiaac, Nortel_7220) were missing from Steel-Belted Radius. (7514)

- When a user loses a VPN connection, the SBR Administrator drops but leaves an active admin session hung. (7507)

- Large service type mapping files would cause severe initialization delays. (7460)

- An issue with RSA New PIN mode prompts has been resolved. (7432)

- Accounting keepalive packets were not supported. (7355)

- Large attribute lists (for example, profiles) could cause heap corruption. (7302)

- Multiple Acct-Delay-Time attributes were added to proxied Accounting-Requests and accounting logs. (7279)

- RADIUS User-name attribute, not EAP user-name, was used when pre-fetching credentials. (7237)

- JRE upgraded to support SMP Multiprocessor Kernel on RedHat Linux. (7212)

- New CRLs were not retrieved during expiration grace period. (7167)

- EAP-NAK would result in Access-Reject rather than use of another method. (7118)

- PEAP/TTLS tunneled user-name was not logged. (7094)

- Session time extension was not correctly returned. (3300)

- **Account lockout**—If you have the lockout feature enabled, you have enabled the TTLS or PEAP method enabled, and you have the Native User, LDAP, or SQL method enabled, then a common outer username, such as **anonymous**, can be locked out, which can deny access to many users. If this occurs:

  1. Open the Order of Methods panel.

  2. Select in turn Native User, LDAP, and SQL (whichever is enabled).

  3. Choose EAP Setup from the context menu.

  4. Check the Handle via Auto-EAP First box. (8456)

- **Hang during shutdown**—If you stop the SBR server and an error occurs when disconnecting from a database or an LDAP server, Steel-Belted Radius may hang. If this occurs, use the **sbrd stop force** command to stop the demon (UNIX) or stop the service (Windows). (249494, old ID-8435)

Documentation Corrections

Steel-Belted Radius Scripting Guide

- `SbrWriteToLog` **method**: The syntax for the SbrWriteToLog method (described on page 79) is incorrect: the optional *logLevel* parameter should precede the message if it is used. The correct syntax is:

  SBRWWriteToLog([*loglevel*,] *msg*)

  For example, the following command writes a message to the Steel-Belted Radius log with a log level of 1:

  SbrWriteToLog(1, "This is an INFORMATIONAL level message");

Steel-Belted Radius Administration Guide (all editions)

- **Missing graphic**: Figure 8 in the *Steel-Belted Radius Administration Guide* was omitted from the PDF file for all editions. The missing graphic appears in Figure 1 on page 16.

Figure 1: Sample rr. File
```
;acme.rr
[Sets]
VPN1=20
VNP2=12
VPN3=7

[VPN1]
Tunnel-Server-Endpoint = 8.4.2.1
Tunnel-Password = GoodGuess

[VPN2]
Tunnel-Server-Endpoint = 8.4.2.2
Tunnel-Password = BestGuess

[VPN3]
Tunnel-Server-Endpoint = 8.4.2.4
Tunnel-Password = OurSecret
```

Upgrade Instructions

Windows/Solaris/Linux: Refer to the *Steel-Belted Radius Installation and Upgrade Guide* for information on upgrading your Steel-Belted Radius software to release 6.1.1.

SBR Appliance: Upgrading the Steel-Belted Radius Appliance to release 6.1.1 is not supported at this time. Refer to the *Steel-Belted Radius Appliance Upgrade Guide* for information on upgrading your Steel-Belted Radius Appliance to Release 5.4.*x*.

List of Technical Publications

The documentation for Steel-Belted Radius consists of the following manuals, which can be downloaded from the Juniper Networks Technical Publications Web page located at http://www.juniper.net/techpubs/software/aaa_802/sbr.html.

- *Steel-Belted Radius Installation and Upgrade Guide*—Describes how to install the Steel-Belted Radius software on a server running the Solaris operating system, the Linux operating system, or the Windows XP/Windows Vista/Windows Server 2003 operating system.

- *Steel-Belted Radius Administration Guide*—Describes how to configure and administer the Steel-Belted Radius server software.

- *Steel-Belted Radius Reference Guide*—Describes the configuration files and settings used by Steel-Belted Radius.

- *Steel-Belted Radius Scripting Guide*—Describes how to use scripts written in the JavaScript programming language to enhance the RADIUS request processing capabilities of the Steel-Belted Radius server.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the Steel-Belted Radius documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at http://www.juniper.net/techpubs/docbug/docbugreport.html. If you are using email, please be sure to include the following information with your comments:

- Documentation name
- Documentation part number
- Software release version
- Page number

Modified Open-Source Software

Embedded in this version of Steel-Belted Radius is open-source software that Juniper Networks, Inc. has modified. The modified software includes:

- LDAP C SDK from The Mozilla Foundation

- HTTPClient from Ronald Tschalär

- **sunmd5.c**, from The OpenSolaris Project

You can obtain the source code for the above modifications by requesting them from Juniper Technical Support.

Contacting Juniper Technical Support

For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

When you are running SBR Administrator, you can choose **Web > Steel-Belted Radius User Page** to access a special home page for Steel-Belted Radius users.

When you call technical support, please have the following at hand:

- Your Steel-Belted Radius edition and release number (for example, Steel-Belted Radius/Global Enterprise Edition Release 6.1.1).

- Information about the server configuration and operating system, including any OS patches that have been applied.

- For licensed products under a current maintenance agreement, your license or support contract number.

- Question or description of the problem, with as much detail as possible.

- Any documentation that may help in resolving the problem, such as error messages, memory dumps, compiler listings, and error logs.